

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-367282
(P2002-367282A)

(43)公開日 平成14年12月20日(2002.12.20)

(51)Int.Cl.⁷
G 1 1 B 20/10
20/14
H 0 4 L 25/49

識別記号
3 4 1

F I
G 1 1 B 20/10
20/14
H 0 4 L 25/49

テ-マコ-ト(参考)
H 5 D 0 4 4
3 4 1 Z 5 K 0 2 9
A

審査請求 未請求 請求項の数35 OL (全 11 頁) + 5

(21)出願番号 特願2001-177571(P2001-177571)

(22)出願日 平成13年6月12日(2001.6.12)

(71)出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者 佐古 曜一郎
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

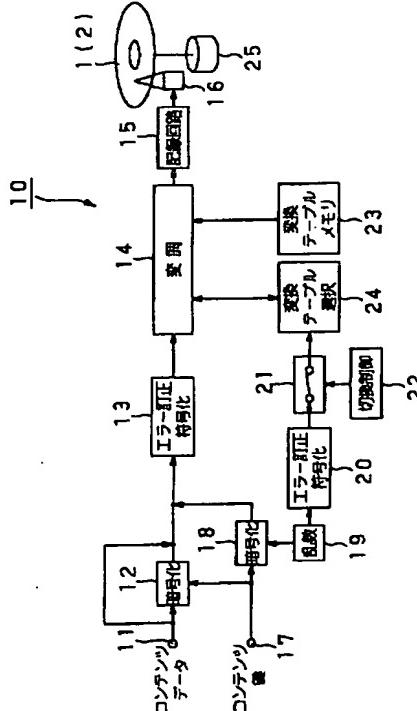
(74)代理人 100067736
弁理士 小池 晃 (外2名)
Fターム(参考) 5D044 AB01 BC04 CC06 DE04 DE29
DE49 DE54 EF03 EF05 FG10
FG18 GK12 GK17 GL20 HH07
HH15
5K029 CC07 GG03

(54)【発明の名称】 データ記録装置及び方法、データ記録媒体、データ再生装置及び方法、データ送信装置及び方法
並びにデータ受信装置及び方法

(57)【要約】

【課題】 秘密データをパーソナルコンピュータ等にそのままコピーされないようにデータをデータ記録媒体に記録し、デジタルデータの不正なコピーを防止する。

【解決手段】 8ビットの主データを16ビットの主データに変調する複数の変換テーブルが格納されたメモリ23と、メモリ23に格納された複数の変換テーブルの中の一を選択し、8ビットの主データを16ビットに変換する変調回路14と、変調回路14で変調された主データを光ディスク1に記録する光ピックアップ16とを備え、変調回路14は、主データとこの主データの付加データが入力されたとき、付加データに従ってメモリ23に格納されている変換テーブルを選択し、主データの変調処理を行い、正規な装置以外では付加データを復調することができないようとする。



【特許請求の範囲】

【請求項1】 m ビットの主データを n ($m < n$) ビットの主データに変調する複数の変換テーブルが格納された格納手段と、

上記格納手段に格納された複数の変換テーブルの中の一を選択し、 m ビットの主データを n ビットに変換する変調手段と、

上記変調手段で変調された主データを記録媒体に記録する記録手段とを備え、

上記変調手段は、主データとこの主データの付加データが入力されたとき、付加データに従って上記格納手段に格納されている変換テーブルを選択し、上記主データの変調処理を行うデータ記録装置。

【請求項2】 上記変調は、8-16変調又は8-10変調である請求項1記載のデータ記録装置。

【請求項3】 上記付加データは、上記主データを暗号化するためのデータである請求項1記載のデータ記録装置。

【請求項4】 上記変調手段は、上記主データの変調前に変換テーブルを選択する請求項1記載のデータ記録装置。

【請求項5】 上記変調手段は、上記付加データに従って上記格納手段に格納されている変換テーブルを選択するとき、上記記録媒体の種類に応じて上記変換テーブルの選択規則を異ならせる請求項1記載のデータ記録装置。

【請求項6】 m ビットの主データとこの主データの付加データが入力されるステップと、

上記付加データに従って、上記 m ビットの主データを n ($m < n$) ビットのデータに変調する複数の変換テーブルの中から一の変換テーブルを選択するステップと、

上記選択した変換テーブルに従って m ビットの主データを n ビットに変調するステップと、

上記変調された主データを記録媒体に記録するステップとを有するデータ記録方法。

【請求項7】 上記変調は、8-16変調又は8-10変調である請求項6記載のデータ記録方法。

【請求項8】 上記付加データは、上記主データを暗号化するためのデータである請求項6記載のデータ記録方法。

【請求項9】 上記主データの変調前に上記変換テーブルを選択する請求項6記載のデータ記録方法。

【請求項10】 上記付加データに従って上記格納手段に格納されている変換テーブルを選択するとき、上記記録媒体の種類に応じて上記変換テーブルの選択規則を異ならせる請求項6記載のデータ記録方法。

【請求項11】 m ビットの主データと共に入力された付加データに従って、 m ビットの主データを n ($m < n$) ビットのデータに変調する複数の変換テーブルの中から一の変換テーブルを選択し、この選択した変換テー

ブルに従って、 m ビットの主データを n ビットのデータに変調したデータが記録されてなるデータ記録媒体。

【請求項12】 上記変調は、8-16変調又は8-10変調である請求項11記載のデータ記録媒体。

【請求項13】 上記付加データは、上記主データを暗号化するためのデータである請求項11記載のデータ記録媒体。

【請求項14】 n ビットの変調された主データを m ($m < n$) ビットの主データに復調するための複数の変換テーブルが格納された格納手段と、

上記 n ビットの主データが上記複数の変換テーブルの中の何れの変換テーブルを用いて変調されたのかを照合する照合手段と、

上記照合手段により照合された変換テーブルに基づいて n ビットの主データを m ビットの主データに復調する復調手段と、

上記照合手段での照合結果より、主データが変調のために何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより上記主データの付加データを生成する生成手段とを備えるデータ再生装置。

【請求項15】 上記変調は、8-16変調又は8-10変調である請求項14記載のデータ再生装置。

【請求項16】 上記付加データは、上記主データを暗号解読するためのデータである請求項14記載のデータ再生装置。

【請求項17】 n ビットの変調された主データを m ($m < n$) ビットの主データに復調するための複数の変換テーブルの中から上記 n ビットの主データが上記複数の変換テーブルの何れを用いて変換されたのかを照合するステップと、

上記照合された変換テーブルに基づいて n ビットの主データを m ビットの主データに復調するステップと、

上記照合結果より、上記主データが変調のため何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより上記主データの付加データを生成するステップとを有するデータ再生方法。

【請求項18】 上記変調は、8-16変調又は8-10変調である請求項17記載のデータ再生方法。

【請求項19】 上記付加データは、上記主データを暗号解読するためのデータである請求項17記載のデータ再生方法。

【請求項20】 m ビットの主データを n ($m < n$) ビットの主データに変調する複数の変換テーブルが格納された格納手段と、

上記格納手段に格納された複数の変換テーブルの中の一を選択し、 m ビットの主データを n ビットに変換する変調手段と、

上記変調手段で変調されたデータを送信する送信手段とを備え、

上記変調手段は、主データとこの主データの付加データ

が入力されたとき、付加データに従って上記格納手段に格納されている変換テーブルを選択し、上記主データの変調処理を行うデータ送信装置。

【請求項21】 上記変調は、8-16変調又は8-10変調である請求項20記載のデータ送信装置。

【請求項22】 上記付加データは、上記主データを暗号化するためのデータである請求項20記載のデータ送信装置。

【請求項23】 上記変調手段は、上記主データの変調前に変換テーブルを選択する請求項20記載のデータ送信装置。
10

【請求項24】 上記変調手段は、上記付加データに従って上記格納手段に格納されている変換テーブルを選択するとき、送信先の装置の種類に応じて上記変換テーブルの選択規則を異ならせる請求項20記載のデータ送信装置。

【請求項25】 mビットの主データとこの主データの付加データが入力されるステップと、

上記付加データに従って、上記mビットの主データをn
20 (m < n) ビットのデータに変調する複数の変換テーブルの中から一の変換テーブルを選択するステップと、

上記選択した変換テーブルに従ってmビットの主データをnビットに変調するステップと、

変調されたデータを送信するステップとを有するデータ送信方法。

【請求項26】 上記変調は、8-16変調又は8-10変調である請求項25記載のデータ送信方法。

【請求項27】 上記付加データは、上記主データを暗号化するためのデータである請求項25記載のデータ送信方法。
30

【請求項28】 上記主データの変調前に上記変換テーブルを選択する請求項25記載のデータ送信方法。

【請求項29】 付加データに従って上記格納手段に格納されている変換テーブルを選択するとき、上記送信先の装置の種類に応じて上記変換テーブルの選択規則を異ならせる請求項25記載のデータ送信方法。

【請求項30】 nビットの変調された主データを受信する受信手段と、

上記受信手段で受信したnビットの変調された主データをm (m < n) ビットの主データに復調するための複数
40 の変換テーブルが格納された格納手段と、

上記nビットの主データが上記複数の変換テーブルの中の何れの変換テーブルを用いて変調されたのかを照合する照合手段と、

上記照合手段により照合された変換テーブルに基づいてnビットの主データをmビットの主データに復調する復調手段と、

上記照合手段での照合結果より、主データが変調のために何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより上記主データの付加データを生
50

成する生成手段とを備えるデータ受信装置。

【請求項31】 上記変調は、8-16変調又は8-10変調である請求項30記載のデータ受信装置。

【請求項32】 上記付加データは、上記主データを暗号解読するためのデータである請求項30記載のデータ受信装置。

【請求項33】 nビットの変調された主データを受信するステップと、

上記受信したnビットの変調された主データをm (m < n) ビットの主データに復調するための複数の変換テーブルの中から上記nビットの主データが上記複数の変換テーブルの何れを用いて変換されたのかを照合するステップと、

上記照合された変換テーブルに基づいてnビットの主データをmビットの主データに復調するステップと、上記照合結果より、上記主データが変調のため何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより上記主データの付加データを生成するステップとを有するデータ受信方法。

【請求項34】 上記変調は、8-16変調又は8-10変調である請求項33記載のデータ受信方法。

【請求項35】 上記付加データは、上記主データを暗号解読するためのデータである請求項33記載のデータ受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データの変調を、複数の変換テーブルを用いてデータを出力するデータ記録装置及びデータ送信装置、変調されたデータが記録されたデータ記録媒体並びに複数の変換テーブルを用いて変調されたデータを復調することができるデータ再生装置及びデータ受信装置に関する。

【0002】

【従来の技術】 ディジタル・バーサタイル・ディスク (以下、digital versatile disc、単にDVDともいう。) は、記録されるデータの著作権保護のために、データがCCS (content scramble system) 等のアクセス制限手段により、スクランブルがかけられて記録されている。このDVDは、再生専用機器で記録データの再生を行うことができる他、パソコンコンピュータ等の汎用機器でも再生することができるようになっている。このような再生機器は、内部メモリに保存された暗号解読キーを用いてDVDに記録されたデータのスクランブルを解除し再生することができるようになっている。

【0003】

【発明が解決しようとする課題】 ところで、DVDに記録されたデータを、パソコンコンピュータ等のハードディスクにそのままコピーし、データのスクランブルを不正に解除することがなされている。これを防止するためには、データのスクランブルを解除するためのデータ

がパーソナルコンピュータ等にそのままコピーされないようにする必要がある。

【0004】本発明の目的は、暗号を解除するためのデータ等の秘密データをパーソナルコンピュータ等にそのままコピーされないようにデータをデータ記録媒体に記録し、ディジタルデータの不正なコピーを防止することができるデータ記録装置及び記録方法、この記録装置及び方法によりデータが記録されたデータ記録媒体並びにこのデータ記録媒体のデータ再生装置を提供することにある。

【0005】また、本発明の目的は、暗号を解除するためのデータ等の秘密データをパーソナルコンピュータ等にそのままコピーされないようにしたデータを送信することができるデータ送信装置及び方法並びにこのデータ送信装置より送信されたデータを受信するデータ受信装置及び方法を提供することにある。

【0006】

【課題を解決するための手段】本発明に係るデータ記録装置は、上述した課題を解決すべく、mビットの主データをn(m<n)ビットの主データに変調する複数の変換テーブルが格納された格納手段と、格納手段に格納された複数の変換テーブルの中の一を選択し、mビットの主データをnビットに変換する変調手段と、変調手段で変調された主データを記録媒体に記録する記録手段とを備える。そして、変調手段は、主データとこの主データの付加データが入力されたとき、付加データに従って格納手段に格納されている変換テーブルを選択し、主データの変調処理を行う。

【0007】また、本発明に係るデータ記録方法は、上述した課題を解決すべく、mビットの主データとこの主データの付加データが入力されるステップと、付加データに従って、mビットの主データをn(m<n)ビットのデータに変調する複数の変換テーブルの中から一の変換テーブルを選択するステップと、選択した変換テーブルに従ってmビットの主データをnビットに変調するステップと、変調された主データを記録媒体に記録するステップとを有する。

【0008】更に、本発明に係るデータ記録媒体は、上述した課題を解決すべく、mビットの主データと共に入力された付加データに従って、mビットの主データをn(m<n)ビットのデータに変調する複数の変換テーブルの中から一の変換テーブルを選択し、この選択した変換テーブルに従って、mビットの主データをnビットのデータに変調したデータが記録されてなる。

【0009】更にまた、本発明に係るデータ再生装置は、上述した課題を解決すべく、nビットの変調された主データをm(m<n)ビットの主データに復調するための複数の変換テーブルが格納された格納手段と、nビットの主データが複数の変換テーブルの中の何れの変換テーブルを用いて変調されたのかを照合する照合手段

と、照合手段により照合された変換テーブルに基づいてnビットの主データをmビットの主データに復調する復調手段と、照合手段での照合結果より、主データが変調のために何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより主データの付加データを生成する生成手段とを備える。

【0010】更にまた、本発明に係るデータ再生方法は、上述した課題を解決すべく、nビットの変調された主データをm(m<n)ビットの主データに復調するための複数の変換テーブルの中からnビットの主データが複数の変換テーブルの何れを用いて変換されたのかを照合するステップと、照合された変換テーブルに基づいてnビットの主データをmビットの主データに復調するステップと、照合結果より、主データが変調のため何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより主データの付加データを生成するステップとを有する。

【0011】更にまた、本発明に係るデータ送信装置は、上述した課題を解決すべく、mビットの主データをn(m<n)ビットの主データに変調する複数の変換テーブルが格納された格納手段と、格納手段に格納された複数の変換テーブルの中の一を選択し、mビットの主データをnビットに変換する変調手段と、変調手段で変調されたデータを送信する送信手段とを備える。そして、変調手段は、主データとこの主データの付加データが入力されたとき、付加データに従って格納手段に格納されている変換テーブルを選択し、主データの変調処理を行う。

【0012】更にまた、本発明に係るデータ送信方法は、上述した課題を解決すべく、mビットの主データとこの主データの付加データが入力されるステップと、付加データに従って、mビットの主データをn(m<n)ビットのデータに変調する複数の変換テーブルの中から一の変換テーブルを選択するステップと、選択した変換テーブルに従ってmビットの主データをnビットに変調するステップと、変調されたデータを送信するステップとを有する。

【0013】更にまた、本発明に係るデータ受信装置は、上述した課題を解決すべく、nビットの変調された主データを受信する受信手段と、受信手段で受信したnビットの変調された主データをm(m<n)ビットの主データに復調するための複数の変換テーブルが格納された格納手段と、nビットの主データが複数の変換テーブルの中の何れの変換テーブルを用いて変調されたのかを照合する照合手段と、照合手段により照合された変換テーブルに基づいてnビットの主データをmビットの主データに復調する復調手段と、照合手段での照合結果より、主データが変調のために何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより主データの付加データを生成する生成手段とを備える。

【0014】更にまた、本発明に係るデータ受信方法は、上述した課題を解決すべく、nビットの変調された主データを受信するステップと、受信したnビットの変調された主データをm(m < n)ビットの主データに復調するための複数の変換テーブルの中からnビットの主データが複数の変換テーブルの何れを用いて変換されたのかを照合するステップと、照合された変換テーブルに基づいてnビットの主データをmビットの主データに復調するステップと、照合結果より、主データが変調のため何れの変換テーブルが使用されたのかをデータとして抽出し、このデータより主データの付加データを生成するステップとを有する。

【0015】

【発明の実施の形態】以下、本発明が適用されたデータ記録媒体、データ記録装置及び記録方法について、図面を参照して説明する。

【0016】本発明が適用されたデータ記録媒体は、記録可能な光ディスクであって、この光ディスク1は、図1に示すように、内周側にTOC(table of contents)等が記録されるリードイン領域1aが設けられ、このリードイン領域1aの外周側に、コンテンツデータが暗号化されて記録されるプログラム領域1bが設けられ、このプログラム領域1bの外周側にリードアウト領域1cが設けられている。また、リードイン領域1aとプログラム領域1bとの間には、プログラム領域1bに記録されるコンテンツデータを暗号化するためのコンテンツ鍵を格納するキーロッカー領域1dが設けられている。このコンテンツ鍵は、記録時に、隠し鍵、例えば乱数によって暗号化され、キーロッカー領域1dに格納されている。

【0017】また、本発明が適用された光ディスクは次のように構成することもできる。この光ディスク2は、図2に示すように、内周側に、第1のセッション3が設けられ、第1のセッション3の外周側に、第2のセッション4が設けられている。各セッション3、4は、それぞれリードイン領域3a、4aが設けられ、リードイン領域3a、4aに次いでプログラム領域3b、4bが設けられ、プログラム領域3b、4bに次いでリードアウト領域3c、4cが設けられている。ここで、第1のセッション3は、標準的な記録密度でデータが記録され、第2のセッション4は、第1のセッション3より記録密度を高くしてデータが記録されている。第2のセッション4のリードイン領域4aとプログラム領域4bとの間には、プログラム領域4bにコンテンツデータを暗号化して記録するためのコンテンツ鍵が格納されるキーロッカー領域4dが設けられている。このコンテンツ鍵は、記録時に、隠し鍵、例えば乱数によって暗号化され、キーロッcker領域に格納されている。以上のような光ディスク2では、例えば外周側の第2のセッション4に、コンテンツデータが記録され、内周側の第1のセッション

10

3には、第2のセッション4に記録されたコンテンツデータの広告データ等が記録されている。また、光ディスク2では、第1のセッション3より第2のセッション4の方に高品質のデータを記録するようにしてもよい。

【0018】次に、本発明が適用されたデータ記録装置10について、図3を参照して説明する。このデータ記録装置10は、入力端子11より入力されたコンテンツデータを暗号化する暗号化回路12と、暗号化回路12で暗号化されたコンテンツデータに対してエラー訂正符号化処理を施すエラー訂正符号化回路13と、エラー訂正符号化処理が施されたコンテンツデータを変調する変調回路14と、変調処理されたコンテンツデータに対して記録処理を施す記録処理回路15と、光ディスク1、2に対してデータを記録する光ピックアップ16と、光ディスク1、2を回転駆動する駆動モータ25とを備える。

20

【0019】また、このデータ記録装置10は、入力端子17より入力されたコンテンツデータを暗号化するためのコンテンツ鍵を暗号化する暗号化回路18と、コンテンツ鍵を暗号化回路18で暗号化するための乱数を発生する乱数発生回路19と、乱数発生回路19が発生した乱数データに対してエラー訂正符号化処理を施すエラー訂正符号化回路20と、エラー訂正符号化処理がされた乱数データの出力を切り換えるスイッチ21と、スイッチ21のオンオフを切り換える切換制御部22と、コンテンツデータを変調するための複数の変換テーブルが格納されたメモリ23と、乱数データに基づいて変調テーブルを選択する変換テーブル選択部24とを備える。

30

【0020】光ディスク1、2に記録するコンテンツデータは、入力端子11より暗号化回路12に入力される。また、入力端子17より入力されたコンテンツデータを暗号化するコンテンツ鍵は、コンテンツデータを暗号化する暗号化回路12に入力される。暗号化回路12は、入力されたコンテンツデータを、コンテンツ鍵を用いて暗号化し、エラー訂正符号化回路13に出力する。なお、光ディスク2の第1のセッション3に記録されるコンテンツデータは、暗号化回路12に入力されること無く、直接エラー訂正符号化回路13に入力される。

40

【0021】また、入力端子17より入力されたコンテンツ鍵は、コンテンツデータを暗号化する暗号化回路12に入力されると共に、コンテンツ鍵を入力する暗号化回路18に入力される。暗号化回路18には、コンテンツ鍵を暗号化する際の隠し鍵となる乱数データ、例えば8ビットのデータ(10100100)が乱数発生回路19より入力される。そして、暗号化回路18は、コンテンツ鍵を乱数データで暗号化した後、乱数で暗号化されたコンテンツ鍵をエラー訂正符号化回路13に入力する。

50

【0022】暗号化された若しくは暗号化されていないコンテンツデータが入力され、また、暗号化されたコン

テンツ鍵のエラー訂正符号化回路13は、入力されたデータに対してCIRC(cross interleaved read-solomon code)等のエラー訂正符号を生成し付加する符号化処理を行う。そして、エラー訂正符号化回路13は、エラー訂正符号化処理がされたデータを、変調回路14に出力する。

【0023】ところで、上述した乱数発生回路19は、コンテンツ鍵を暗号化するために乱数を発生し、この乱数データを、コンテンツ鍵を暗号化する暗号化回路18に出力すると共に、光ディスク1,2に乱数データを記録するための処理を行うため、エラー訂正符号化回路20に出力する。そして、乱数データが入力されたエラー訂正符号化回路20は、乱数データに対してエラー訂正符号化処理を行う。そして、エラー訂正符号化回路20は、乱数データを、光ディスク1,2に記録するため、スイッチ21を介して変換テーブル選択部24に出力する。スイッチ21は、切換制御部22にオンオフが切り換えられるものであり、切換制御部22は、光ディスク1,2のキーロッカー領域1d,4dに暗号化されたコンテンツ鍵を記録するときに限ってスイッチ21をオンとし、エラー訂正符号化処理が施された乱数を変換テーブル選択部24に出力することができるようとする。

【0024】変調回路14は、入力されたデータに対して例えば8-16変調処理を行う。メモリ23には、8-16変調処理を行うための複数の変換テーブルが格納されている。具体的に、メモリ23に格納された変換テーブルは、図4に示すように、8ビットの入力データを16ビットに変換するコードテーブルを4つ有している。この変換テーブル30は、各8ビットの入力データに対して次に用いるコードテーブルナンバが定められている。

【0025】また、メモリ23には、図5に示すように、図4に示した変換テーブルの補助テーブルが格納されている。この補助テーブルは、例えば上記図4に示した変換テーブルを用いて8-16変調を行うと、DSV(digital sum variation)の絶対値が所定値以上となってしまうとき、DSVを所定値未満とするために用いられる。この補助テーブルも、8ビットの入力データを16ビットに変換するコードテーブルを4つ有しており、各8ビットの入力データに対して次に用いるコードテーブルナンバが定められている。

【0026】変調回路14は、通常、すなわち、コンテンツデータを変調するとき、図4に示す変換テーブルを用い、この変換テーブルに規定された規則に従ってコードテーブル1~4を選択する。例えば、変調回路14は、図4に示すように、入力コードナンバが2の8ビットデータを、コードテーブル1を用いて16ビットのデータに変換したとき、次の8ビットのデータを、コードテーブル2を用いて16ビットのデータに変換する。ま

た、変調回路14は、DSVを所定値未満とするため図5に示す補助変換テーブルを選択したときにも、コンテンツデータを変調するとき、この補助変換テーブルを用い、この補助変換テーブルに規定された規則に従ってコードテーブル1~4を選択する。そして、変調回路14は、変調したコンテンツデータを記録処理回路15に出力する。

【0027】また、変調回路14は、光ディスク1,2のキーロッカー領域1d,4dに暗号化したコンテンツ鍵を記録するとき、次のように動作する。先ず、変調回路14には、エラー訂正符号化処理がなされた暗号化されたコンテンツ鍵がエラー訂正符号化回路13より入力される。また、キーロッcker領域1d,4dに暗号化したコンテンツ鍵を記録するとき、切換制御部22は、スイッチ21をオンとし、変換テーブル選択部24には、エラー訂正符号化回路20からエラー訂正処理がなされた乱数データが入力される。

【0028】変換テーブル選択部24は、乱数データに基づいて、例えば上記図4及び図5に示す変換テーブルに規定された変調規則と異なった規則で、図4に示す変換テーブルと図5に示す変換テーブルを選択する。すなわち、変換テーブル選択部24は、復調時に、図4に示す変換テーブルと図5に示す変換テーブルの選択そのものが、乱数データとなるように変換テーブルを選択する。

【0029】また、変換テーブル選択部24は、図4、図5に示す変換テーブルの選択に際して、ランレンジングスが(RLL(2,10))、すなわち0の最小ランが2で最大ランが10となるように図4、図5に示す変換テーブルを選択する。更に、変換テーブル選択部24は、DSVが所定値以上とならないように図4、図5に示す変換テーブルを選択する。

【0030】そして、変換テーブル選択部24は、選択した変換テーブルとコードテーブルナンバを変調回路14に出力する。そして、変調回路14は、メモリ23に格納されている変換テーブルに基づいて暗号化されたコンテンツ鍵を変調する。また、変調回路14は、変換テーブル選択部24が次に用いる図4、図5に示す変換テーブルを、ランレンジングスが(RLL(2,10))でDSVが所定値以上とならないように選択することができるよう、現在変調に使用した変換テーブルの種類とコードテーブルナンバを、変換テーブル選択部24に出力する。そして、変換テーブル選択部24は、上述したように、乱数データに基づいて、次に用いる図4、図5に示す変換テーブルを選択する。そして、変調回路14は、変調したコンテンツ鍵を記録処理回路15に出力する。そして、記録処理回路15は、変調されたコンテンツデータやコンテンツ鍵のデータの2値化等の記録処理を行い、光ピックアップ16に出力する。

【0031】光ピックアップ16は、モータ25で例え

ばCLV (constant linear velocity) で回転されている光ディスク1, 2の信号記録面に光ビームを照射して、データを記録する。具体的に、光ピックアップ16は、リードイン領域1a, 3a, 4aにTOC等を記録し、キーロッカー領域1d, 4dに、コンテンツ鍵を記録し、プログラム領域1b, 3b, 4bに、コンテンツデータを記録する。特に、光ディスク2のプログラム領域4bには、記録密度を高めてコンテンツデータが記録される。

【0032】以上のようなデータ記録装置10によって記録された光ディスク1, 2は、既存のデータ再生装置で再生するとき、キーロッカー領域1d, 4dに格納されているコンテンツ鍵が通常と異なる規則で変調されていることから、このコンテンツ鍵を復調することができない。したがって、光ディスク1, 2は、権限の無いデータ再生装置で、暗号化されているコンテンツデータが再生されることを防止することができる。すなわち、このようにコンテンツ鍵が記録された光ディスク1, 2では、パーソナルコンピュータ等にそのままコピーされたときであっても、暗号化されているコンテンツ鍵が復調されることが無くなり、また、コンテンツ鍵を暗号化するための乱数データを抽出することもできないことから、不正に、コンテンツ鍵の暗号が解読されコンテンツデータの暗号も解読されてしまうことを防止することができる。

【0033】以上の例は、コンテンツ鍵の変調の際して、変換テーブルの選択の規則を異ならせる例を説明したが、コンテンツ鍵の代わりにダミーデータを乱数データに基づいて、図4又は図5に示す変換テーブルを用いて行うようにしてもよい。この場合、変換テーブル選択部24は、乱数データそのものをコードテーブルナンバに変換し、これに基づいて変調回路14がダミーデータを変調するようすればよい。また、変換テーブル選択部24は、乱数データに基づいて図4若しくは図5の変換テーブルのコードテーブルナンバの偶数と奇数を選択し、これに基づいて変調回路14がダミーデータを変調するようすればよい。勿論、ダミーデータを、乱数データに基づいて図4に示す変換テーブルと図5に示す変換テーブルを選択し、選択した変換テーブルに基づいて変調を行うようにしてもよい。なお、この場合、コンテンツ鍵は、キーロッカー領域1d, 4dに格納しており、ダミーデータは、キーロッカー領域1d, 4dの領域、すなわち光ディスク1のリードイン領域1a、プログラム領域1b、リードアウト領域1cに記録し、また、光ディスク2のリードイン領域3a, 4a、プログラム領域3b, 4b、リードアウト領域3c, 4cに記録しておくようとする。

【0034】次に、以上のようなデータ記録装置10によってデータが記録されたデータ再生装置30について、図6を参照して説明する。このデータ再生装置30 50

は、光ディスク1, 2を回転するモータ31と、光ディスク1, 2に記録されたデータの読み出しを行う光ピックアップ32と、光ピックアップ32からデータを增幅するRFアンプ33と、モータ31と光ピックアップ32のサーボ制御をするサーボ回路34と、RF信号からTOC等を抽出するサブコード抽出部35と、RFアンプ33から入力されたコンテンツデータやコンテンツ鍵を復調する復調回路36と、復調されたデータのエラー訂正処理を行うエラー訂正復号化回路37と、暗号化されているデータを解読する暗号解読回路38とを備える。また、データ再生装置30は、データの復調を行った際に用いる変換テーブルが格納されたメモリ39と、変調に用いられた変換テーブルを照合する照合部40と、コンテンツ鍵の暗号を解読するための乱数データを抽出するための抽出部41と、照合部40からのデータを選択的に抽出部41に出力するようにするためのスイッチ42と、抽出部41で抽出した乱数データをエラー訂正処理を行うエラー訂正復号化回路43と、スイッチ42等全体の動作を制御する制御部44とを備える。

【0035】光ピックアップ32は、モータ32により例えばCLVで回転している光ディスク1, 2に光ビームを照射し、戻りの光ビームを検出し、光電変換した後、RFアンプ33に出力する。RFアンプ33は、光ピックアップ32から電気信号が入力されると、RF信号を生成すると共に、フォーカシングエラー信号とトラッキングエラー信号を生成する。そして、RFアンプ33は、復調回路36に出力し、フォーカシングエラー信号とトラッキングエラー信号をサーボ回路34に出力する。サーボ回路34は、フォーカシングエラー信号とトラッキングエラー信号に基づいてフォーカスサーボ信号とトラッキングサーボ信号を生成し、光ピックアップ32に出力する。これにより、光ピックアップ32は、対物レンズのフォーカシング及びトラッキング制御を行う。また、サーボ回路34は、モータ31のサーボ信号を生成しモータ31に出力し、モータ31は、サーボ制御される。サブコード抽出部35は、RFアンプ33より出力されたRF信号よりサブコードを抽出し、TOC等を制御部44に出力する。

【0036】復調回路36は、8-16変調されたデータを復調する。ここで、メモリ39には、上記図4に示した変換テーブルと図5に示した補助変換テーブルが格納されている。制御部44は、キーロッカー領域1d, 4dの読み出しを行うと判断したとき、コンテンツ鍵の暗号化している乱数データの抽出を行うため、スイッチ42をオンにする。そして、照合部40は、図7に示すように、ステップS1において、RFアンプ33よりRF信号が入力されると、ステップS2において、入力された暗号化されたコンテンツ鍵のデータが図4に示した変換テーブルと図5に示した補助変換テーブルを用いて変調されているかを判断する。ここで、照合部40は、

照合結果、すなわち変調に用いられた変換テーブルの種類を変調回路14に出力し、変調回路14は、照合部40からの入力に基づいて、メモリ39に格納されている図4に示した変換テーブルと図5に示した補助変換テーブルに基づいてコンテンツ鍵を復調し、エラー訂正復号化回路37に出力する。

【0037】これと共に、照合部40は、ステップS3において、入力された暗号化されたコンテンツ鍵のデータが図4に示す変換テーブルを用いて変調されたのかどうかを判断する。そして、照合部40は、図4に示す変換テーブルが用いられたと判断したとき、ステップS4において、「1」を抽出部41に出力し、図4に示す変換テーブルが用いられていないと判断したとき、ステップS5において、「0」を抽出部41に出力する。そして、制御部44は、サブコード抽出部35から入力されたアドレス情報に基づいてキーロッカー領域1d, 4dのデータ読み出しが終了したと判断したとき、スイッチ42をオフとし、コンテンツ鍵の読み出しを終了し、データの読み出しが終了していないとき、ステップS1からの処理を繰り返す。

【0038】コンテンツ鍵の変調に際して用いられた変換テーブルの選択データが「1」又は「0」として入力された抽出部41は、ステップS7において、入力されたデータからコンテンツ鍵を暗号化したときの乱数データを抽出する。そして、抽出部41は、乱数データをエラー訂正符号化回路43に出力し、エラー訂正符号化回路43は、乱数データのエラー訂正処理を行い、エラー訂正処理がされた乱数データを暗号解読回路に出力する。

【0039】一方、エラー訂正復号化回路37は、復調回路36より復調された暗号化されたコンテンツ鍵が入力されると、これをエラー訂正処理し、暗号解読回路38に出力する。暗号解読回路38は、エラー訂正符号化回路43から入力された乱数データに基づいて、エラー訂正符号化回路37から入力されたコンテンツ鍵の暗号解読を行う。そして、暗号解読回路38は、暗号化されているコンテンツデータの暗号解読を行うことができるよう、暗号解読されたコンテンツ鍵を図示しないメモリ等に保存する。

【0040】次いで、光ディスク1のプログラム領域1bや光ディスク2のプログラム領域4bに暗号化されて記録されているコンテンツデータを読み出すとき、復調回路36は、暗号化されているコンテンツデータを、通常の規則に従って復調する。そして、復調されたコンテンツデータは、エラー訂正符号化回路37でエラー訂正処理がなされ、次いで、暗号解読回路38に入力される。暗号解読回路38は、暗号解読したコンテンツ鍵を用いてコンテンツデータの暗号解読を行う。そして、暗号解読回路38は、出力端子45に出力する。出力端子45には、モニタやスピーカが接続されており、暗号解

読されたコンテンツデータは、映像であればモニタに表示され、音声データであればスピーカより出力される。

【0041】以上のようなデータ再生装置30は、データ記録装置10によってデータが記録された光ディスク1, 2の再生を行うことができる。すなわち、データ再生装置30は、キーロッカー領域1d, 4dに格納された通常と異なる規則で変調されたコンテンツ鍵を復調することができる。ここで、このデータ再生装置30は、既存の図4及び図5に示す変換テーブルを有していることから、従来の光ディスクとの互換を図ることもできる。

【0042】なお、コンテンツ鍵の代わりにダミーデータを乱数データに基づいて、図4又は図5に示す変換テーブルを用いて変調した場合の復調方法について説明する。

【0043】先ず、コードテーブルナンバが乱数データであるとき、図8に示すように、制御部44がダミーデータが記録された領域の読み出しを開始するとき、制御部44は、スイッチ42をオンの状態とし、先ず、ステップS11において、照合部40には、ダミーデータが入力される。ステップS12において、照合部40は、ダミーデータを変調する際に用いた図4又は図5に示すコードテーブルナンバを抽出する。ステップS13において、照合部40で抽出されたコードテーブルナンバは、抽出部41に入力される。そして、抽出部41は、コードテーブルナンバよりコンテンツ鍵の暗号を解読するのに必要な乱数データを生成する。そして、抽出部41は、暗号解読回路38に出力する。一方、復調回路36は、通常の規則に従って、キーロッカー領域1d, 4dに格納されているコンテンツ鍵を復調し、エラー訂正符号化回路37は、このコンテンツ鍵のエラー訂正処理を行う。そして、暗号解読回路38は、コンテンツ鍵の暗号を、乱数データに基づいて解読する。そして、暗号解読回路38は、暗号化されたコンテンツデータが入力されたとき、暗号解読したコンテンツ鍵を用いて、コンテンツデータの暗号解読を行い、出力端子45よりコンテンツデータを出力する。

【0044】また、コードテーブルナンバの偶奇によつて乱数データを表現しているとき、図9に示すように、制御部44がダミーデータが記録された領域の読み出しを開始するとき、制御部44は、スイッチ42をオンの状態とし、先ず、ステップS21において、照合部40は、RFアンプ33よりRF信号が入力されると、ステップS22において、照合部40は、ダミーデータを変調する際に用いた図4又は図5に示すコードテーブルナンバを抽出する。そして、抽出部41は、ステップS23において、コードテーブルナンバが偶数であるか奇数であるかの判断を行う。そして、ステップS24において、照合部40は、コードテーブルナンバが偶数であるとき、「1」を抽出部41に出力し、ステップS25に

において、コードテーブルナンバが奇数であるとき、「0」を抽出部41に出力する。そして、制御部44は、サブコード抽出部35から入力されたアドレス情報に基づいてダミーデータが記録された領域の読み出しが終了したと判断したとき、スイッチ42をオフとし、コンテンツ鍵の読み出しを終了し、データの読み出しが終了していないとき、ステップS21からの処理を繰り返す。そして、コードテーブルナンバの偶奇が「1」又は「0」として入力された抽出部41は、ステップS27において、入力されたデータからコンテンツ鍵を暗号化したときの乱数データを抽出する。そして、抽出部41は、乱数データをエラー訂正符号化回路43に出力し、エラー訂正符号化回路43は、乱数データのエラー訂正処理を行い、エラー訂正処理がされた乱数データを暗号解読回路に出力する。一方、復調回路36は、通常の規則に従って、キーロックカ一領域1d, 4dに格納されているコンテンツ鍵を復調し、エラー訂正符号化回路37は、このコンテンツ鍵のエラー訂正処理を行う。そして、暗号解読回路38は、コンテンツ鍵の暗号を、乱数データに基づいて解読する。そして、暗号解読回路38は、暗号化されたコンテンツデータが入力されたとき、暗号解読したコンテンツ鍵を用いて、コンテンツデータの暗号解読を行い、出力端子45よりコンテンツデータを出力する。

【0045】以上、記録可能の光ディスクを例に取り説明したが、再生専用の光ディスクに適用することもできる。また、本発明は、光ディスクの種類、すなわち再生専用形光ディスク、追記形光ディスク、書換形光ディスクとで変調の規則を変えるようにしてもよい。また、以上、8-16変調を例に取り説明したが、この他に、8-10変調等であってもよい。また、以上の例では、コンテンツデータを暗号化するコンテンツ鍵を主データとし、このコンテンツ鍵を暗号化する乱数データを付加データとして説明したが、例えば、主データをコンテンツデータとし、付加データをコンテンツデータを暗号化するコンテンツ鍵としてもよい。

【0046】また、本発明は、上述したデータ記録装置10で記録するデータをデータ受信装置に送信する送信装置に適用することもできる。また、本発明は、このデータ送信装置より送信されたデータを受信し復調するデータ受信装置に適用することもできる。

【0047】

【発明の効果】本発明は、主データの変調を、付加データに基づいて変換テーブルを選択して行うようにし、再生を行うとき、主データが変調のため何れの変換テーブル

10

* ルが使用されたのかをデータとして抽出し、このデータより上記主データの付加データを生成するようにしている。したがって、既存の装置では、主データの再生を行うことができるが、付加データの再生を行うことができないようになることができる。例えば、主データをコンテンツデータとし、このコンテンツデータを付加データである暗号鍵で暗号化したとき、この暗号鍵を、既存の装置では、取得することができないようにし、再生することができないようにすることができる。すなわち、正規な装置でのみ、コンテンツデータの暗号を解読し再生することができるようになることができる。

【図面の簡単な説明】

【図1】光ディスクの構成を説明する図である。

【図2】光ディスクの他の例を説明する図である。

【図3】データ記録装置のブロック図である。

【図4】8-16変調を行うためのメイン変換テーブルを説明する図である。

【図5】8-16変調を行うための補助変換テーブルを説明する図である。

【図6】光ディスクのデータ再生装置を説明する図である。

【図7】乱数データを抽出する手順を説明するフローチャートである。

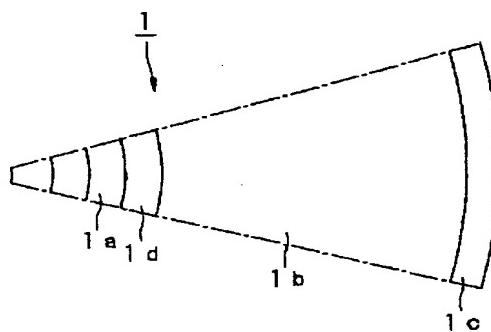
【図8】コードナンバより乱数データを抽出する手順を説明するフローチャートである。

【図9】コードナンバの偶奇より乱数データを抽出する手順を説明するフローチャートである。

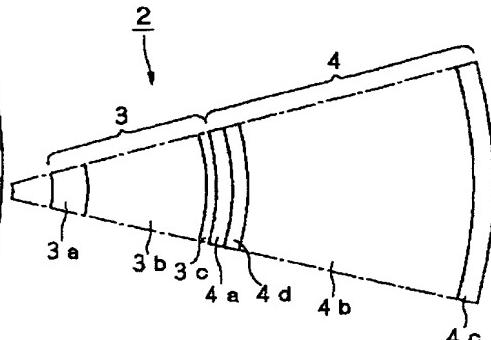
【符号の説明】

- 1 光ディスク、2 光ディスク、3 第1のセッション、4 第2のセッション、1a, 3a, 4a リードイン領域、1b, 3b, 4b プログラム領域、1c, 3c, 4c リードアウト領域、1d, 4d キーロックカ一領域、10データ記録装置、11 入力端子、12 暗号化回路、13 エラー訂正符号化回路、14 変調回路、15 記録処理回路、16 光ピックアップ、17 入力端子、18 暗号化回路、19 乱数発生回路、20 エラー訂正符号化回路、21 スイッチ、22 切換制御部、23 メモリ、24 変換テーブル選択部、30 データ再生装置、31 モータ、32 光ピックアップ、33 RFアンプ、34 サーボ回路、35 サブコード抽出部、36 復調回路、37 エラー訂正復号化回路、38 暗号解読回路、39 メモリ、40 照合部、41 抽出部、43 エラー訂正復号化回路、44 制御部、45 出力端子

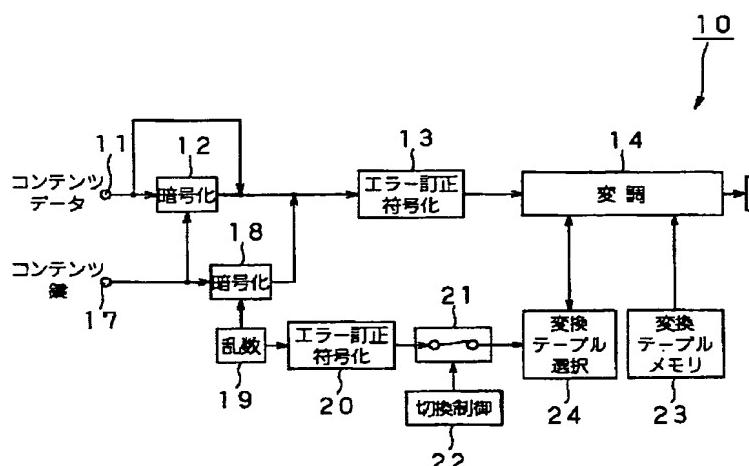
【図1】



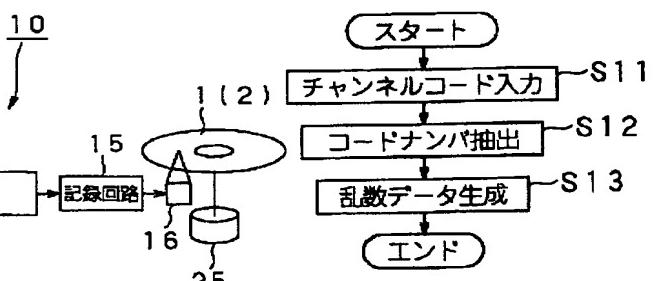
【図2】



【図3】



【図8】



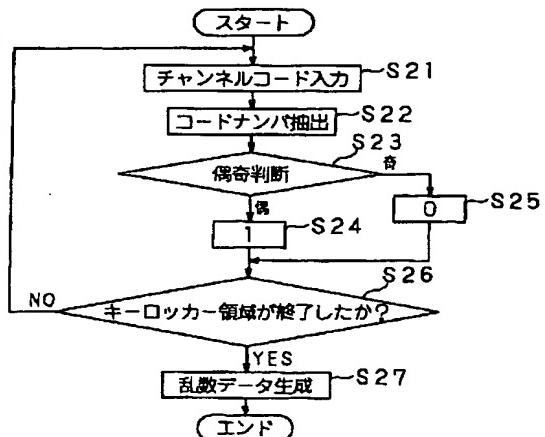
【図4】

8ビット入力 データ(コー ドナンバ)	コードテーブル1		コードテーブル2		コードテーブル3		コードテーブル4	
	出力データ (16ビット)	次のコー ドテーブ ルナンバ	出力データ (16ビット)	次のコー ドテーブ ルナンバ	出力データ (16ビット)	次のコー ドテーブ ルナンバ	出力データ (16ビット)	次のコー ドテーブ ルナンバ
0	0010---	1	0100---	2	0010---	1	0100---	2
1	0010---	1	0010---	1	1000---	3	1000---	3
2	0010---	2	0010---	2	1000---	1	1000---	1
3	0010---	2	0100---	4	0010---	2	0100---	4
.
.
255

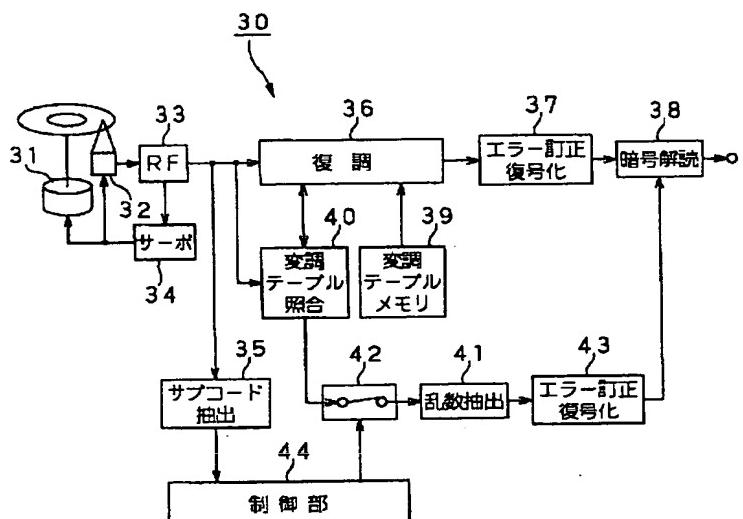
メインテーブル

【图5】

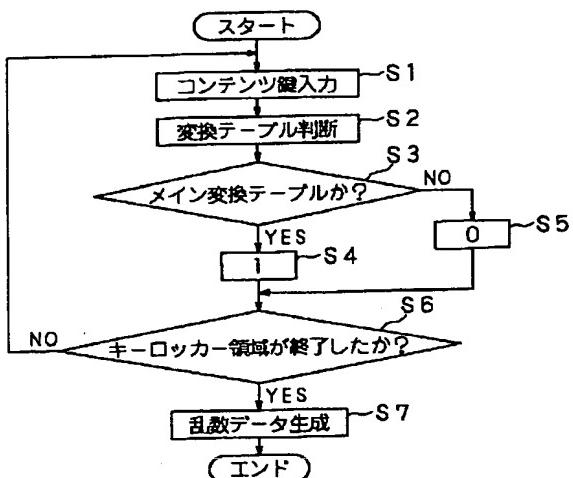
[図 9]



〔四六〕



【图 7】



【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第4区分

【発行日】平成15年6月20日(2003.6.20)

【公開番号】特開2002-367282(P2002-367282A)

【公開日】平成14年12月20日(2002.12.20)

【年通号数】公開特許公報14-3673

【出願番号】特願2001-177571(P2001-177571)

【国際特許分類第7版】

G11B 20/10

20/14 341

H04L 25/49

【F I】

G11B 20/10 H

20/14 341 Z

H04L 25/49 A

【手続補正書】

【提出日】平成15年3月4日(2003.3.4)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正内容】

【発明の名称】記録媒体の記録装置及び記録方法、記録媒体の再生装置及び再生方法、データ出力方法並びにデータ復号方法、

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】mビットのデータをn(m < n)ビットのデータに変換するための複数の変換テーブルが記憶された記憶部と、記録媒体に記録されるmビットのデータの種類によって上記記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換える選択制御部と、上記選択制御部によって選択された変換テーブルを用いて、入力されたmビットのデータをnビットのデータに変調する変調処理部と、

上記変調処理部からの出力データを記録媒体に記録する記録部とを備えている記録媒体の記録装置。

【請求項2】上記選択制御部は、上記mビットのデータを暗号化する際に用いられたデータに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項1記載の記録媒体の記録装置。

【請求項3】上記装置は、更に乱数データに基づいて上記mビットのデータに暗号化処理を施す暗号化回路部

を備え、上記選択制御部は上記乱数データに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項2記載の記録媒体の記録装置。

【請求項4】上記選択制御部は、上記記録媒体に暗号化されたmビットのコンテンツデータを記録する場合と上記記録媒体に上記暗号化する際に用いられたmビットの鍵データを記録する場合とで上記記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換える請求項1記載の記録媒体の記録装置。

【請求項5】上記選択制御部は、上記記録媒体に上記暗号化されたコンテンツデータを記録するときには信号の直流成分が所定の値より小さくなるように所定の規則に従って上記記憶部に記憶されている複数の変換テーブルを選択し、上記記録媒体に上記鍵データを記録するときには上記所定の規則とは異なる規則に従って上記記憶部に記憶されている複数の変換テーブルを選択する請求項4記載の記録媒体の記録装置。

【請求項6】上記装置は、更に乱数データに基づいて上記mビットの鍵データに暗号化処理を施す暗号化回路部を備え、上記選択制御部は上記乱数データに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項5記載の記録媒体の記録装置。

【請求項7】上記変調処理部は、mは8でnが16である8-16変調方式に基づいて変調処理を行う請求項1記載の記録媒体の記録装置。

【請求項8】記録媒体にデータを記録する際に、上記記録媒体に記録されるデータの種類に基づいて、mビットのデータをn(m < n)ビットに変換するための複数の変換テーブルが記憶された記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換え、

上記選択された変換テーブルを用いて、入力されたmビットのデータをnビットのデータに変調し、

上記変調されたデータを記録媒体に記録する記録媒体の記録方法。

【請求項9】 上記方法は、上記mビットのデータを暗号化する際に用いられたデータに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項8記載の記録媒体の記録方法。

【請求項10】 上記方法は、更に乱数データに基づいて上記mビットのデータに暗号化し、上記乱数データに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項9記載の記録媒体の記録方法。

【請求項11】 上記方法は、上記記録媒体に暗号化されたmビットのコンテンツデータを記録する場合と上記記録媒体に上記暗号化する際に用いられたmビットの鍵データを記録する場合とで上記記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換える請求項8記載の記録媒体の記録方法。

【請求項12】 上記方法は、上記記録媒体に上記暗号化されたコンテンツデータを記録するときには信号の直流成分が所定の値より小さくなるように所定の規則に従って上記記憶部に記憶されている複数の変換テーブルを選択し、上記記録媒体に上記鍵データを記録するときには上記所定の規則とは異なった規則に従って上記記憶部に記憶されている複数の変換テーブルを選択する請求項11記載の記録媒体の記録方法。

【請求項13】 上記方法は、更に乱数データに基づいて上記mビットの鍵データに暗号化し、上記乱数データに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項12記載の記録媒体の記録方法。

【請求項14】 上記方法における変調処理は、mは8でnが16である8-16変調方式に基づいて変調処理を行う請求項8記載の記録媒体の記録方法。

【請求項15】 nビットのデータが記録された記録媒体からデータを読み出すヘッド部と、
mビットのデータをn(m< n)ビットのデータに変換するための複数の変換テーブルが記憶された記憶部と、
上記記録媒体に記録されるnビットのデータの種類によって上記記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換える選択制御部と、
上記選択制御部によって選択された変換テーブルを用いて、上記ヘッド部からの出力信号に基づくnビットのデータをmビットのデータに復調する復調処理部とを備えている記録媒体の再生装置。

【請求項16】 上記選択制御部は、上記ヘッド部からの出力信号に基づくnビットのデータの変調処理の際に用いられた変調用の変換テーブルの種類を判別する照合部とを備え、上記選択制御部は上記照合部による判別結果に基づいて上記復調処理部に上記変換テーブルを選択するための選択制御信号を供給する請求項15記載の記録媒体の再生装置。

【請求項17】 上記装置は、更に上記照合部による照

合結果に基づいて上記nビットのデータに施されている暗号化を解くためのデータを抽出する抽出部と上記抽出部によって抽出された暗号化を解くためのデータを用いて上記復調処理部からの出力データの暗号を解読する暗号化解読部とを備えている請求項16記載の記録媒体の再生装置。

【請求項18】 上記記録媒体には、nビットの暗号化されたコンテンツデータと上記コンテンツデータの暗号を解くためのnビットの暗号化された鍵データとが記録されており、上記選択制御部は、上記記録媒体からnビットのコンテンツデータを読み出すときには、所定の規則に従って上記記憶部に記憶されている複数の変換テーブルいずれかの変換テーブルを選択し、上記記録媒体から上記鍵データを読み出すときには上記照合部による判別結果に基づいて上記変換テーブルを選択する請求項16記載の記録媒体の再生装置。

【請求項19】 上記装置は、先ず上記記録媒体に記録されている上記暗号化された鍵データを読み出し、上記選択制御部は上記照合部による判別結果に基づいて上記復調処理部に上記変換テーブルを選択するための選択性制御信号を供給し、上記暗号化された鍵データを復調する請求項16記載の記録媒体の再生装置。

【請求項20】 上記装置は、更に上記照合部による照合結果に基づいて上記暗号化された鍵データの暗号化を解くためのデータを抽出し、上記抽出された暗号化を解くためのデータを用いて上記復調処理部から出力される暗号化された鍵データの暗号を解読する請求項19記載の記録媒体の再生装置。

【請求項21】 上記装置は、上記解読された鍵データを用いて上記復調処理部から出力された暗号化されたコンテンツデータの暗号を解読する請求項20記載の記録媒体の再生装置。

【請求項22】 上記復調処理部は、mは8でnが16である8-16変調方式に基づいて復調処理を行う請求項20記載の記録媒体の再生装置。

【請求項23】 記録媒体から読み出されたnビットのデータの種類によって、nビットのデータをm(m< n)ビットのデータに変換するための複数の変換テーブルが記憶された記憶部に記憶された複数の変換テーブルの選択の仕方を切り換え。

上記選択された変換テーブルを用いて、上記読み出されたnビットのデータをmビットのデータに復調する記録媒体の再生方法。

【請求項24】 上記方法は、上記記録媒体から読み出されたnビットのデータの変調処理の際に用いられた変調用の変換テーブルの種類を判別照合し、上記照合結果に基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項23記載の記録媒体の再生方法。

【請求項25】 上記方法は、更に上記照合結果に基づいて上記nビットのデータに施されている暗号化を解く

ためのデータを抽出し、上記抽出された暗号化を解くためのデータを用いて上記復調されたデータの暗号を解読する請求項24記載の記録媒体の再生方法。

【請求項26】 上記記録媒体には、nビットの暗号化されたコンテンツデータと上記コンテンツデータの暗号を解くためのnビットの暗号化された鍵データとが記録されており、上記方法は、上記記録媒体からnビットのコンテンツデータを読み出すときには、所定の規則に従って上記記憶部に記憶されている複数の変換テーブルいずれかの変換テーブルを選択し、上記記録媒体から上記鍵データを読み出すときには上記照合結果に基づいて上記変換テーブルを選択する請求項24記載の記録媒体の再生方法。

【請求項27】 上記方法は、先ず上記記録媒体に記録されている上記暗号化された鍵データを読み出し、上記照合結果に基づいて上記変換テーブルを選択するための選択性制御信号を供給し、上記暗号化された鍵データを復調する請求項24記載の記録媒体の再生方法。

【請求項28】 上記方法は、更に上記照合結果に基づいて上記暗号化された鍵データの暗号化を解くためのデータを抽出し、上記抽出された暗号化を解くためのデータを用いて上記復調された暗号化された鍵データの暗号を解読する請求項27記載の記録媒体の再生方法。

【請求項29】 上記方法は、上記解読された鍵データを用いて上記復調された暗号化されたコンテンツデータの暗号を解読する請求項28記載の記録媒体の再生方法。

【請求項30】 上記方法における復調処理は、mは8でnが16である8-16変調方式に基づいて復調処理を行う請求項23記載の記録媒体の再生方法。

【請求項31】 データを出力する際に、上記出力されるデータの種類に基づいて、mビットのデータをn(m < n)ビットのデータに変換するための複数の変換テーブルが記憶された記憶部に記憶された複数の変換テーブルの選択の仕方を切り替え、

上記選択された変換テーブルを用いて、上記読み出されたmビットのデータをnビットのデータに変調し、上記変調されたデータを出力するデータ出力方法。

【請求項32】 上記方法は、上記mビットのデータを暗号化する際に用いられたデータに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項31記載のデータ出力方法。

【請求項33】 上記方法は、更に乱数データに基づいて上記mビットのデータを暗号化し、上記乱数データに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項32記載のデータ出力方法。

【請求項34】 上記方法は、上記暗号化されたmビットのコンテンツデータを出力する場合と上記コンテンツデータを暗号化する際に用いられたmビットの鍵データを出力する場合とで上記記憶部に記憶されている複数の

変換テーブルの選択の仕方を切り換える請求項31記載のデータ出力方法。

【請求項35】 上記方法は、上記暗号化されたコンテンツデータを出力ときには信号の直流成分が所定に値よりも小さくなるように所定の規則に従って上記記憶部に記憶されている複数の変換テーブルを選択し、上記鍵データを出力するときには上記所定の規則とは異なった規則に従って上記記憶部に記憶されている複数の変換テーブルを選択する請求項34記載のデータ出力方法。

【請求項36】 上記方法は、更に乱数データに基づいて上記mビットの鍵データに暗号化し、上記乱数データに基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項35記載のデータ出力方法。

【請求項37】 上記方法における変調処理は、mは8でnが16である8-16変調方式に基づいて変調処理を行う請求項31記載のデータ出力方法。

【請求項38】 供給されたnビットのデータの種類によって、nビットのデータをm(m < n)ビットのデータに変換するための複数の変換テーブルが記憶された記憶部に記憶された複数の変換テーブルの選択の仕方を切り替え、上記選択された変換テーブルを用いて、上記読み出されたnビットのデータをmビットのデータに復調するデータ復号方法。

【請求項39】 上記方法は、上記nビットのデータの変調処理の際に用いられた変調用の変換テーブルの種類を判別照合し、上記照合結果に基づいて上記記憶部に記憶されている複数の変換テーブルを選択する請求項38記載のデータ復号方法。

【請求項40】 上記方法は、更に上記照合結果に基づいて上記nビットのデータに施されている暗号化を解くためのデータを抽出し、上記抽出された暗号化を解くためのデータを用いて上記復調されたデータの暗号を解読する請求項39記載のデータ復号方法。

【請求項41】 上記方法は、上記nビットのコンテンツデータを復調するときには、所定の規則に従って上記記憶部に記憶されている複数の変換テーブルのいずれかの変換テーブルを選択し、上記鍵データを復調するときには上記照合結果に基づいて上記変換テーブルを選択する請求項39記載のデータ復号方法。

【請求項42】 上記方法は、先ず上記暗号化された鍵データを復調するために、上記照合結果に基づいて上記変換テーブルを選択するための選択性制御信号を供給し、上記暗号化された鍵データを復調する請求項39記載のデータ復号方法。

【請求項43】 上記方法は、更に上記照合結果に基づいて上記暗号化された鍵データの暗号化を解くためのデータを抽出し、上記抽出された暗号化を解くためのデータを用いて上記復調された暗号化された鍵データの暗号を解読する請求項42記載のデータ復号方法。

【請求項44】 上記方法は、上記解読された鍵データ

を用いて上記復調された暗号化されたコンテンツデータの暗号を解読する請求項4.3記載のデータ復号方法。

【請求項4.5】 上記方法における復調処理は、 m は8で n が16である8-16変調方式に基づいて復調処理を行う請求項3.8記載のデータ復号方法。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正内容】

【0001】

【発明の属する技術分野】本発明は、データの変調を、複数の変換テーブルを用いてデータを出力する記録媒体の記録装置及び記録方法、変調されたデータが記録された記録媒体の再生装置及び再生方法、データ出力方法並びにデータ復号方法に関する。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正内容】

【0006】

【課題を解決するための手段】上述した目的を達成するために提案される本発明に係る記録媒体の記録装置は、 m ビットのデータを n ($m < n$) ビットのデータに変換するための複数の変換テーブルが記憶された記憶部と、記録媒体に記録される m ビットのデータの種類によって記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換える選択制御部と、選択制御部によって選択された変換テーブルを用いて、入力された m ビットのデータを n ビットのデータに変調する変調処理部と、変調処理部からの出力データを記録媒体に記録する記録部とを備えている。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0007

【補正方法】変更

【補正内容】

【0007】また、本発明に係る記録媒体の記録方法は、記録媒体にデータを記録する際に、上記記録媒体に記録されるデータの種類に基づいて、 m ビットのデータを n ($m < n$) ビットに変換するための複数の変換テーブルが記憶された記憶部に記憶されている複数の変換テーブルの選択の仕方を切り替え、選択された変換テーブルを用いて、入力された m ビットのデータを n ビットのデータに変調し、この変調されたデータを記録媒体に記録する。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正内容】

【0008】本発明に係る記録媒体の再生装置は、 n ビットのデータが記録された記録媒体からデータを読み出すヘッド部と、 m ビットのデータを n ($m < n$) ビットのデータに変換するための複数の変換テーブルが記憶された記憶部と、記録媒体に記録される n ビットのデータの種類によって記憶部に記憶されている複数の変換テーブルの選択の仕方を切り換える選択制御部と、選択制御部によって選択された変換テーブルを用いて、ヘッド部からの出力信号に基づく n ビットのデータを m ビットのデータに復調する復調処理部とを備えている。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正内容】

【0009】本発明に係る記録媒体の再生装置は、更に照合部による照合結果に基づいて n ビットのデータに施されている暗号化を解くためのデータを抽出する抽出部とこの抽出部によって抽出された暗号化を解くためのデータを用いて復調処理部からの出力データの暗号を解読する暗号化解読部とを備えている。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正内容】

【0010】本発明に係る再生装置によって再生される記録媒体には、 n ビットの暗号化されたコンテンツデータとコンテンツデータの暗号を解くための n ビットの暗号化された鍵データとが記録されており、選択制御部が、記録媒体から n ビットのコンテンツデータを読み出すときには、所定の規則に従って記憶部に記憶されている複数の変換テーブルいずれかの変換テーブルを選択し、記録媒体から鍵データを読み出すときには照合部による判別結果に基づいて変換テーブルを選択する。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正内容】

【0011】本発明に係る記録媒体の再生方法は、記録媒体から読み出された n ビットのデータの種類によって、 n ビットのデータを m ($m < n$) ビットのデータに変換するための複数の変換テーブルが記憶された記憶部に記憶された複数の変換テーブルの選択の仕方を切り替え、選択された変換テーブルを用いて、読み出された n ビットのデータを m ビットのデータに復調する。

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正内容】

【0012】本発明は、データ出力方法であり、データを出力する際に、出力されるデータの種類に基づいて、 m ビットのデータを n ($m < n$) ビットのデータに変換するための複数の変換テーブルが記憶された記憶部に記憶された複数の変換テーブルの選択の仕方を切り換え、選択された変換テーブルを用いて、読み出された n ビットのデータを m ビットのデータに復調する。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正内容】

【0013】本発明は、データ復号方法であり、供給された n ビットのデータの種類によって、 n ビットのデータを m ($m < n$) ビットのデータに変換するための複数の変換テーブルが記憶された記憶部に記憶された複数の変換テーブルの選択の仕方を切り換え、選択された変換テーブルを用いて、読み出された n ビットのデータを m ビットのデータに復調する。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正内容】

【0014】本発明に係るデータ復号方法は、 n ビットのデータの変調処理の際に用いられた変調用の変換テーブルの種類を判別照合し、その照合結果に基づいて記憶部に記憶されている複数の変換テーブルを選択し、更に照合結果に基づいて n ビットのデータに施されている暗号化を解くためのデータを抽出し、抽出された暗号化を解くためのデータを用いて復調されたデータの暗号を解読する。